In the Claims:

Amend Claims 1, 7, 13, 17, 24,27,28,31, 34 as follows:

1. (currently amended) A system for authenticating an encryption key of a user at a ~~remote~~ client ~~computer~~ computing device that may be ~~remotely~~ networked to a server computer, comprising: a decrypt engine in the ~~remote~~ client computer for using a password provided by the user to decrypt in the ~~remote~~ client computer an encrypted data file provided by the user so as to form a decrypted data file and so as to use the decrypted data file to form at least port of the ~~encryption~~ key of the user, without transmitting to the server either the password, the encrypted data file or the decrypted data file

7. (~~previously~~ currently amended) A method for providing an authenticated encryption key of a user at a ~~remote~~ client ~~computer~~ computing device that may be ~~remotely~~ networked to a server computer comprising the steps of:

providing an encrypted data file to the ~~remote~~ client computer;

providing a password to the ~~remote~~ client computer; and

decrypting the encrypted data file in the ~~remote~~ client computer using the password so as to generate an authenticated encryption key of the user without transmitting the server either the password or, the encrypted data file.

13. (currently amended) A computer accessible medium comprising program instructions for providing at a ~~remote~~ client ~~computer~~ computing device that may be ~~remotely~~ networked to a server computer an authenticated ~~encryption~~ user key ~~of a user~~, comprising the steps of: using a password provided by the user to decrypt in the ~~remote~~ client computer an encrypted data file provided by the user so as to form a decrypted data file and so as to use the decrypted data file to form at least part of an authenticated ~~encryption~~ key of the user, without transmitting to the server either the password, the encrypted data file or the decrypted data file

17. (currently amended) A system for authenticating an encryption key of a user, comprising: an input device at a ~~remote~~ client ~~computer~~ computing device that may be ~~remotely~~ networked to a server computer for receiving a password provided by the user at the ~~remote~~ client computer ~~remotely~~ that may be networked to a server computer; memory in the ~~remote~~ client

~~computer~~ computing device for storing an encrypted data file including an encryption key of the user; and a decrypt engine in the ~~remote~~ client computer for using the password to decrypt the encrypted data file so as to form a decrypted data file and so as to use the decrypted data file to generate in the ~~remote~~ client computer an authenticated ~~encryption~~ key of a user, without transmitting to the server either the password, the encrypted data file or the decrypted data file

24. (currently amended) A system for authenticating an encryption key of a user at a ~~remote~~ client ~~computer~~ computing device that may be ~~remotely~~ networked to a server computer, comprising: an input device at the ~~remote~~ client computer for receiving a password provided by the user; an RF smart card for storing an encrypted data file, the encrypted data file ~~including~~ being the encrypted source of ~~an encryption~~ a user key ~~of user~~; a decrypt engine in the ~~remote~~ client computer for using the password to decrypt the encrypted data file to generate in the ~~remote~~ client computer an authenticated ~~encryption~~ key of the user, without transmitting to the server either the password, the encrypted data file or the decrypted data file; memory in the ~~remote~~ client computer for storing the decrypt engine.

27. (currently amended) A system for authenticating an encryption key of a user at a ~~remote~~ client ~~computer~~ computing device that may be ~~remotely~~ networked to a server computer, comprising: an input device at the ~~remote~~ client computer for receiving a password provided by the user; an RF smart card for storing an encrypted data file, the encrypted data file being the encrypted source of a user key~~the encrypted data file including an encryption key of the user~~ and containing first biometric data of the user; a biometric reader for generating second biometric data of the user; a decrypt engine in the ~~remote~~ client computer for using the password to decrypt the encrypted data file so as to form a decrypted data file to generate in the ~~remote~~ client computer an authenticated ~~encryption~~ key of the user, if there is a probabalistic match between the first biometric data and the second biometric data without transmitting to the server either the password, the encrypted data file or the decrypted data file;

28. (currently amended) A system for authenticating an encryption key of a user at a ~~remote~~ client ~~computer~~ computing device that may be ~~remotely~~ networked to a server computer, comprising: memory in the ~~remote~~ client computer for storing an encrypted encryption key; an input device at the ~~remote~~ client computer for receiving a password; a decrypt engine in

the ~~remote~~ client computer for using the password to decrypt the encrypted data file so as to form a decrypted data file to generate in the ~~remote~~ client computer an authenticated encryption key of the user without transmitting to the server either the password, the encrypted data file or the decrypted data file; memory in the client computer for storing the decrypt engine without transmitting to the server either the password, the encrypted data file or the decrypted data file.

31. (currently amended) A system for authenticating an encryption key of a user at a ~~remote~~ client ~~computer~~ computing device that may be ~~remotely~~ networked to a server computer, comprising: memory in the ~~remote~~ client computer for storing an encrypted encryption key and a first biometric data of the user; an input device at the ~~remote~~ client computer for receiving a password; a biometric reader at the ~~remote~~ client computer for generating a second biometric data of the user; a decrypt engine in the ~~remote~~ client computer for comparing the first biometric data of the user with a second biometric data of the user and, if there is a probabilistic match, then using the password to decrypt the encrypted encryption key without transmitting to the server either the password, the encrypted data file or the decrypted data file, data of the user.

34. (currently amended) A method for authenticating an encryption key of a user at a ~~remote~~ client ~~computer~~ computing device that may be ~~remotely~~ networked to a server computer, comprising the steps of: storing an encrypted key in memory in a remote computer; receiving a password provided by the user; and requiring use of the password in the remote computer to decrypt the encrypted encryption key so as to form a decrypted encryption key without transmitting to the server either the password or the encrypted encryption key.